UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,409	12/04/2003	Richard C. Johnson	ORCL5881	7705

53156 7590 12/08/2006

YOUNG LAW FIRM, P.C.
4370 ALPINE RD.
STE. 106
PORTOLA VALLEY, CA 94028

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 12/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/727,409	JOHNSON, RICHARD C.	
	Examiner	Art Unit	
	Charlie C. Agwumezie	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-13,15-19 and 29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-13, 15-19and 29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/17/03; 8/15/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 25, 2006 has been entered.

Status of Claims

1. Claims 6, 14, and 20-28, are cancelled.

Claims 1, 9, 15, and 29 are amended.

Claims 1-5, 7-13, 15-19, and 29-33, are pending in this application per the request for continued examination filed on September 25, 2006.

Response to Arguments

2. Applicant's arguments with respect to claim 1-5, 7-13, 15-19, and 29-33, have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-8 and 29-33**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of Hwangbo U.S. Patent Application Publication No. 2003/0154376 A1 and further in view of Fischer U.S. Patent No. 5,214,702.

13. As per **claims 1 and 29**, Brown et al discloses in a computing environment having a connection to a network, computer readable code readable by a computer system in said environment, for enabling a server computer within the computing environment to both authenticate a user of a client computer within the computing environment and to verify that the user is authorized to request that the server computer carry out a requested action, comprising:

a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field;

wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate by accessing a store of authority information that is independent of digital certificate (see figs. 1 and 3; 0165; 0067; 0174; 0183) by accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information.

What brown does not explicitly teach is a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field; and

accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information.

Hwangbo discloses a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field (fig. 10; 0029; 0034; 0096; claim 17).

Fischer discloses accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information (fig. 3; see claim 1. 17, 20 and 41)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured to enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field and matching the authority of a user within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information in view of the teachings of Hwangbo and Fischer respectively in order to show details and/or configurable nature of X.509 and its capabilities.

14. As per **claim 2 and 30,** Brown et al further discloses a computer readable code, wherein the digital certificate conforms to the X.509 standard (0109; 0164; 0183).

15. As per **claim 3 and 31**, Brown et al further discloses the computer readable code, wherein the second code portion is configured as XML code (0062; 0068; 0069).

16. As per **claim 4 and 32**, Brown et al further discloses the computer readable code, wherein the XML code is compliant with a DSML standard (0109; 0164; 0183).

17. As per **claim 5 and 33**, Brown et al further discloses the computer readable code, wherein the authority of the user of the client computer is stored in a hierarchical authority data structure that is accessible by the server computer (0183).

18. As per **claim 6**, Brown et al further discloses the computer readable code, wherein the authority of the user defined within the second code portion of the certificate is verifiable by the server computer accessing a store of authority information that is independent of the received certificate (0183).

19. As per **claim 7**, Brown et al further discloses the computer readable code, wherein the authority defined within the second code portion defines access rights of the user to data and programs within the computing environment (0183).

20. As per **claim 8**, Brown et al further discloses the computer readable code, wherein the authority defined within the second code portion defines rights of the user to issue payment requests (0183; see claim 80).

Claims 9-13, and 15-19, are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of in view of Fischer U.S. Patent No. 5,214,702.

5. As per **claim 9**, Brown et al discloses a computer-implemented method for ensuring non-repudiation of a payment request, the payment request being generated in a computing environment having a connection to a network, the method comprising the steps of:

receiving, over the network, the payment request together with a certificate identifying a user having caused the payment request to be generated, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information defining an authority of the user to make the payment request (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

validating the certificate-identifying information and the user-identifying information included within the received certificate by accessing a store of authority information that is independent of the received certificate (figs. 1, 2, 3, and 8; 0165; 0067; 0174; 0183; claim 80);

validating the authority information included within the received certificate, by accessing a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information, and

executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80)

What Brown does not explicitly teach is validating the authority information included within the received certificate, by accessing a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information.

Fischer discloses accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information (fig. 3; see claim 1. 17, 20 and 41)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a method of accessing, over the network, a store of authority information that is independent of the

digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information as taught by Fischer, in order to ensure adequate security during validation.

6. As per **claim 10**, Brown et al further discloses the method, wherein the payment request is for a predetermined amount and wherein the payment request is authorized only when the validating steps are successful and when the authority information for the user stored in the hierarchical authority data structure lists an authorized amount for the user at least equal to the predetermined amount (0177; 0183; 0184; 0185).

7. As per **claim 11 and 16**, Brown et al further discloses the method, wherein the certificate received in the receiving step conforms to the X.509 standard (0109; 0164; 0183).

8. As per **claim 12 and 17**, Brown et al further discloses the method, wherein the authority information is configured as XML code (0062; 0068; 0069).

9. As per **claim 13 and 18**, Brown et al further discloses the method, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

10. As per **claim 15**, Brown et al discloses a software application configured to carry

out a financial transaction, the application being configured to run on a computer coupled to a network, and comprising, stored on a computer-readable medium:

certificate receiving code which is configured to receive a digital certificate from a user over the network, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information that defines an authority granted to the user to request that the financial transaction be carried out (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

certificate validating code configured to enable validation of the certificate-identifying information and user-identifying information within the received certificate (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

What Brown does not explicitly teach is

authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is coupled to the network and that is independent of the received certificate by accessing the data structure over the network and by matching the authority information included in the received certificate to the corresponding authority information stored in the accessed data structure.

Fischer discloses authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is coupled to the network and that is independent of the received certificate by accessing the data structure over the network and by matching the authority information included in the received certificate to

the corresponding authority information stored in the accessed data structure (fig. 3; see claim 1. 17, 20 and 41).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a method of authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is coupled to the network and that is independent of the received certificate by accessing the data structure over the network and by matching the authority information included in the received certificate to the corresponding authority information stored in the accessed data structure.

11. As per **claim 19**, Brown et al further discloses the software application, wherein the authority defined by the authority information within the received certificate also defines rights of the user to access predetermined data and programs within the network (0183; 0184).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The reference cited to Skibbie et al U.S. Patent No. 6,910,128 is a document considered relevant to the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on **(571) 272 – 6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington D.C. 20231

Or faxed to:

(571) 273-8300. [Official communications; including After Final communications labeled "Box AF"].

(571) 273-8300. [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"].

Hand delivered responses should be brought to the United States Patent and Trademark Office Customer Service Window:

Randolph Building,

401 Dulany Street

Alexandria VA. 22314

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621
December 1, 2006

KAMBIZ ABDI
PRIMARY EXAMINER
3621